Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 29 April 2019 – Friday 17 May 2019

Supervised hours: 4 hours	Paper Reference **20158K**

Information Technology

Unit 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this paper is 37.

Turn over ▶

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour, **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner’s work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 21 May 2019.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand in your work to your teacher/tutor.

Set Task Brief

Projet Serendipity

Projet Serendipity (PS) is an independent, non-profit organisation formed in 2018, which tries to make links between PhD students. Its joint Chief Executives are Professor Fred Gorse, an expert in artificial intelligence, and Professeur Adele Lefebvre, who studies complex data processing.

PS was formed for PhD students to work on computing projects. It now involves over 20 universities around the world and has several PhD students working with it.

PS occupies four rooms on the second floor of a building owned by the Pan-Europe Foundation for Education Research (PEFER), based in Lille, France. PS has meeting rooms and workspace but most PhD students work from home, accessing the servers and data stores remotely.

The PS board is elected from present PhD students and their supervisors. Fred and Adele provide oversight and continuity, other board members deal with the day-to-day running of PS and its research programme.

Client brief

You advised Fred and Adele on cyber security matters. Now, six months later, Adele has asked you to review the investigation of a cyber security incident.

Three months ago Adele saw an article on the MondeLePlusÉtrange.fr ('Strangest World' in English) website. The article was about a coincidental link between different areas of science and had obviously been written about some of PS's work.

A week later another article appeared, and then another the following week. Each one based on PS's work.

Adele discussed the matter with Fred and they decided to investigate. In particular to find if MondeLePlusÉtrange was accessing that information from the PS network.

The investigation team was:

- Professeur Adele Lefebvre
- Mlle Marina Maubour, a PhD student living in Lille
- M. Anton Bernoul, the senior IT Manager at PEFER.

The investigation took 10 days, during which time two more articles appeared on MondeLePlusÉtrange. The articles then stopped and no more have been published.

The investigation was inconclusive, although several security matters were addressed during it. Adele believes that whoever was involved was scared off by the investigation.

Evidence items from the security incident at PS

Evidence items include:

1) Adele’s account
2) Marina’s report
3) Report from PEFER’s senior IT Manager
4) WiFi map and notes
5) Cyber security document – incident management policy.

1 Adele’s account

> PS had only been in its new location for a few weeks when a friend emailed me the URL of an article in MondeLePlusÉtrange. The article was about an unexpected link between two different areas of science. My friend knew about PS and thought I’d be interested.
>
> I wasn’t expecting much. MondeLePlusÉtrange is mainly ‘click-bait’. Its articles are mostly true but twist ordinary events into something that sounds sensational. The headline on the article was ‘Astounding Coincidence!!! You’ll never guess how these two things are linked’.
>
> Anyway, I had a look and really was astounded, the material was something we’d discovered at PS only the previous month. There were no names and the whole thing was vague as to when or where it had happened, but I recognised it straight away.
>
> I raised the matter at our next board meeting, two days later. We decided that there was not much we could do. Perhaps one of our research students had talked about their work, or someone had overheard something. It could even have been an independent discovery, although it seemed unlikely that it would be announced through MondeLePlusÉtrange.
>
> I emailed MondeLePlusÉtrange, explaining PS, and asked to meet the author to discuss the article. MondeLePlusÉtrange replied saying they never reveal sources, the author was a staff journalist, and they did not wish to discuss the matter.
>
> Then three more articles were published, one a week. We were certain by then that someone was getting information from PS, so we started an investigation. It was still possible that a student had talked, but we didn’t think that anyone could have been involved with everything in all three articles.
>
> I was nominally in charge of the investigation but the work was mainly done by Anton and Marina. The articles finally stopped after number five. By that time the investigation was being talked about by everyone in PS and I think we scared off whoever was involved.

2 Marina’s report

Adele asked me to represent PS in the investigation. I live in Lille and often work in the building and I get on well with Anton. I have a good idea of how the PS system works, but I’m no expert with cyber security, so Anton and his team did the technical bits.

Anton asked me to help by:

a. Taking a WiFi signal reader and my smartphone to find where I could locate the PS WiFi and log in, both inside and outside the building. There was a good signal inside as expected but it was difficult to get a reliable connection outside. I’ve drawn a map **(see evidence item 4)** that Anton has used in his report.

b. Checking the computer files to see when relevant files were last accessed. That was inconclusive. I knew which research had been referenced by the articles and I’m sure that none of the more obvious files had been looked at recently. Things like progress reports and grant applications. The problem is that data files get used all the time, so it was impossible to say if there had been unauthorised access. All the data is encrypted, so I don’t think anyone could have used them even if they did get into the data stores.

c. Checking the paper files. To see what files had been updated recently. They might have been left on a desk or in the printer for a visitor to see. There were several relevant files, all of them progress reports. Most would have been used at the previous board meeting, or sent in support of grant applications. Someone would have been in the building when they were printed but it’s possible that the documents could have been unattended for a while. They’re not really that secret. Anton checked the print dates against the PEFER visitor log but didn’t find anything.

3 Report from PEFER's senior IT Manager, M. Anton Bernoul

Investigation into a possible data breach at Projet Serendipity (PS)

At the request of Professeur Adele Lefebvre, I looked into ways in which information might have been obtained from PS. I investigated six routes.

a) PEFER and PS personnel
b) Visitors
c) Malware
d) The PS WiFi system
e) Software faults and misconfiguration
f) Hardware faults and misconfiguration

a) PEFER and PS personnel

PEFER. All of our staff, academic and service, have been with PEFER for at least three years. There have been no similar incidents with PEFER data. I think it impossible that any member of the academic staff is involved. I think it extremely unlikely that any of the service staff are involved. A possible route might be if someone put documents in the general waste rather than shredding it.

PS. Professeur Lefebvre has stated that she does not think that all of the students handling the materials referred to in the articles could have been overheard, or have left papers laying around. The PEFER security log shows that most students had not been in the building in the month before the first article.

b) Visitors

The PEFER security log for the month before the first article shows all the visitors had made an appointment. All visitors were escorted to the correct room by a member of the security staff.

c) Malware

My team scanned the PS system, including the backup store and any mobile devices and portable storage devices that were available. Nothing was found.

d) The PS WiFi system **NETGEAR ProSAFE WAC730 using 802.11ac**

I asked Mlle Maubour to survey WiFi signals in the building and surrounding area. She reported that she could get a signal for some distance but no reliable connection at more than a few metres from the building. Her map is included **(see evidence item 4)**.

The outside of the PEFER building is covered by CCTV, so I think it unlikely that an attacker would risk being seen on the street and the area is a no parking zone. It is possible that someone was in a nearby building, such as one of the cafes, but Mlle Maubour could not log in from that distance.

e) Software faults and misconfiguration

All system software had the latest patches and I could not find any configuration errors.

f) Hardware faults and misconfiguration

No physical faults were found but two other issues were identified.

(i) The WiFi access point had not been patched since 2017, it seems to have been missed out when the system was set up. I don't think there have been any WPA2 vulnerabilities found since then, but I cannot be certain. I reset the WAP to factory settings and then patched everything up to the latest versions. I also made the password more secure. I thought Projet2019 was a bit flimsy.

(ii) The router, Cisco 7200. I left a network monitoring tool running for a couple of days to see if there was any suspicious traffic. I was surprised to find that the router itself was sending a signal at 0200 each morning. I checked again over several days to make sure. The signal went to 29.101.211.195 and seemed to be an attempt to report in. There was no reply. I pinged the address and got this:

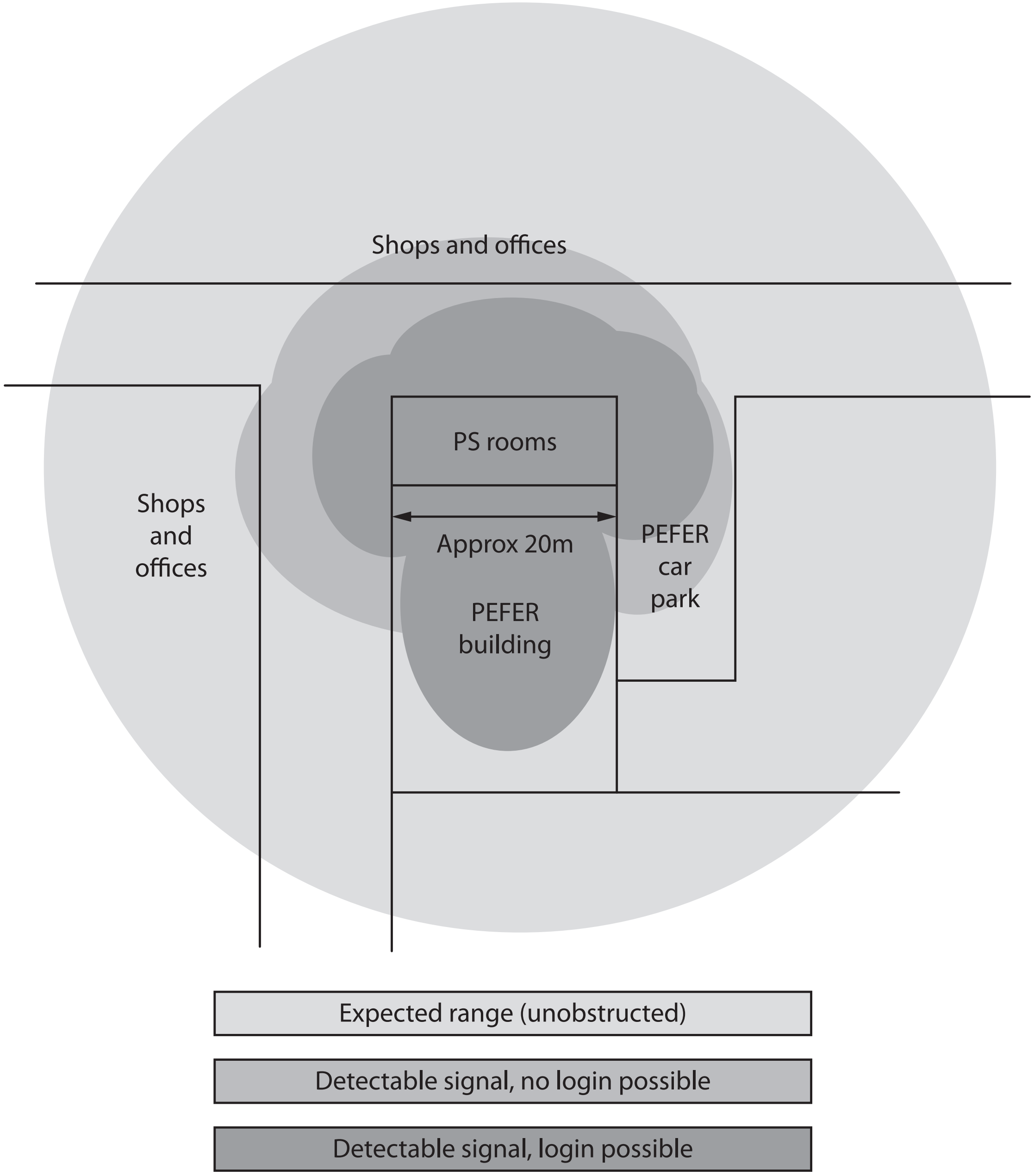
```
PING 29.101.211.195 (29.101.211.195) 56(84) bytes of data.

--- 29.101.211.195 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

The 29 address means it's a class A network that belongs to the Defense Information Systems Agency.

The router firmware is the latest available version and the router has been out of support since 2015, so I don't think there is much to be done except perhaps change the router.

4 WiFi map and notes


Shops and offices
Shops
and
offices
PS rooms
Approx 20m
PEFER
building
PEFER
car
park
Expected range (unobstructed)
Detectable signal, no login possible
Detectable signal, login possible

Notes:

i. Coverage lobes estimated from Mlle Maubour's measurements. There could be up to a 5m error in coverage shown

ii. CCTV covers the three sides of the building but only for 5m from the wall. The car park has complete CCTV coverage.

5 Cyber security documentation – Incident Management Policy

Incident Management Policy

Incident Management Team
Computer Security Incident Response Team (CSIRT) will be:
Professor F Gorse and / or Professeur A Lefebvre
Older member, available from the PEFER IT team
One or more members of the Projet Serendipity board

Event reports

Some employee who thinks that an IT security incident has occurred should report it as soon as possible to the head of the CSIRT (Computer Security Incident Response Team).
Initially, it can be reported orally, but it must be followed by an email.
The CSIRT is responsible for keeping detailed documentation of the incident from the first report to the final solution. Security incidents can include:
Theft of PS equipment
Theft of PS data
Unauthorised access to the PS's computer systems
Infecting the PERER's computer systems with malware.

Incident Response Procedure
a) Theft of computer equipment
Theft of computer equipment is a very serious problem. All thefts must be reported to the CSIRT official immediately. As a first step, an oral report must be prepared, followed by an email with as much information as possible (location and type of equipment, date of last visit, etc.).
The CSIRT team leader needs to check if the item was actually stolen (or just missing).
If the theft is confirmed, CSIRT's team leader must inform the police and contact the finance department to inform the insurers.
The CSIRT must provide the directors with a report of the theft and, where appropriate, justify the finances required to replace the stolen item.

b) Theft of PS data
The theft or loss of PERER's data equipment can be done in several ways. Any loss of PS data must be reported immediately to the head of the CSIRT team, as a first step, and must be followed by an oral report by email.
The CSIRT must investigate the loss and pinpoint what data was lost or stolen, and when the incident took place.
After identifying what has been lost or stolen and when, the CSIRT needs to restore the backups and recover the data as soon as possible.
The CSIRT should review the incident and implement procedures to prevent future losses.

c) Unauthorised access to PS systems
Employees suspecting unauthorised access to a computer system must immediately report this to the CSIRT team leader, specifying as much detail as possible (which system has been accessed). First, an oral report must be prepared, followed by an email.
The CSIRT will conduct a thorough investigation of the incident and determine how unauthorised access has occurred.
The CSIRT will take all necessary measures to prevent future events (e.g. change passwords).

d) Infection of PS computer systems with malware
Employees who suspect that a computer system has been infected with malware must immediately report to the CSIRT Team Leader. As a first step, an oral report must be sent by email.
The infected system should be shut down as soon as possible.
The CSIRT will examine the infection and take appropriate action to correct the infection and restore the system.

Part B Set Task

You must complete ALL activities in the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Projet Serendipity on cyber security. Now, six months later, you have been called in to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Projet Serendipity.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–4 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–5 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS